Part 1:

Answer the following questions by clearly circling the *most appropriate* answer [1 mark each]

1. True or False: Digital signatures provide the ability to authenticate message content but does not authenticate message source.
   a. True
   b. False

2. True or False: Cryptographic hash functions are required to be one-way and collision-resistant.
   a. True
   b. False

3. In public key cryptography if *X* wants to send an encrypted confidential message to *Y*
   a. *X* encrypts message using his private key
   b. *X* encrypts message using *Y*'s private key
   c. *X* encrypts message using *Y*'s public key
   d. *X* encrypts message using his public key

4. Message authentication codes (MAC) and digital signatures both serve to authenticate the content of a message. Which of the following best describes how they differ?
   a. A MAC can be verified based only on the message, but a digital signature can only be verified with the secret key used to sign the message.
   b. A MAC can be verified based only on the message, but a digital signature can only be verified with the public key of the party that signed the message.
   c. A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified based only on the message.
   d. A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified with the public key of the party that signed the message.

5. Which of the following is <u>not</u> a many-to-one function for message *M*
   a. MAC (*M*, *K*)
   b. Hash (*M*)
   c. RSA_Encryption (*M*, *e*, *n*) , where *e* and *n* are the public key
   d. Digital Signature (*M*)

6. On many occasions, systems have been broken not because of a poor encryption algorithm, but because of poor key selection or management. Which of the following is a desirable action to the above matter
   a. frequent key changes
   b. frequent encryption algorithm changes
   c. Use multiple encryption algorithms
   d. Use multiple hash algorithms

7. A digital signature is required
   i. to tie an electronic message to the sender's identity
   ii. for non repudiation of communication by a sender
   iii. to prove that a message was sent by the sender in a court of law
   iv. in all e-mail transactions

   a. i and ii
   b. i, ii, iii
   c. iii, iv
   d. ii, iv

8. The responsibility of a certification authority (CA) for digital signature is to authenticate the

   a. hash function used
   b. private keys of subscribers
   c. public keys of subscribers
   d. key used in DES

9. Which of the following is **not** an SSL protocol

   a. SSL handshake protocol
   b. SSL change cipher Spec protocol
   c. SSL record protocol
   d. SSL session protocol

10. HTTPS refers to

   a. The HTTP and SSL handshake that allows the server and client to authenticate each other and to negotiate encryption
   b. The HTTP and SSL establishment of security capabilities by the client to initiate and establish capabilities
   c. The combination of HTTP and SSL to implement secure communication between a web browser and a web server.
   d. The HTTP-specific protocol to change of pending state to be copied into current state

Part 2:

1. Suppose that Alice chooses for an RSA system the primes $p = 61$, and $q = 41$, and the public key $e = 7$. [3 marks]

   (a) Write the equation to encrypt the plaintext $M = 254$. $C = M^e \bmod n$

   $n = p \cdot q = (61 * 41)$

   $\phi(n) = (p-1)(q-1) = 60 * 40 = 2400$

   $C = 254^7 \bmod (61 * 41)$ $PU = \{e, n\}$

   (b) Write the equation to decrypt the ciphertext C=545 with d = 343

   $M = C^d \bmod n$

   $= 545^{343} \bmod (61 * 41)$

   $PR = \{d, n\}$

   3

2. In RSA key setup, assume p=3 , q=11 and e=7. Compute the public and private keys: [3 marks]

   $PU = \{e, n\}$, $PR = \{d, n\}$

   $n = p \cdot q = 33$

   $\phi(n) = (p-1)(q-1) = 20$

   $e \cdot d \bmod \phi(n) = 1 \Rightarrow d = 3$

   $PU = \{7, 33\}$

   $PR = \{3, 33\}$

   3

3. In RSA, why primes p,q must not be easily derived from modulus n=p.q [1 point]

   because if we can derive p and q then we can calculate $\phi(n)$ and find value of d, so we get the private key.

   1

4. Alice chooses for an RSA system the primes $p = 7$, and $q = 11$, and the public key $e = 7$ to encrypt message M=88. What is wrong with the RSA setup (beside using small numbers): [1 mark]

   because the message is larger than n (88 > 77)

   1

5. Why public key cryptography was developed? List two issues resolved by public key [2 points]

   ① we can key distribution easly, "the public key".

   ② to achive non-repudation of ~~origin~~ sender of the message.

   2

Part 3:

1. List four ways of distributing public keys. [2 points]

i. Public Announsment ii. Public Available directory

ii. Public-key Authirty iv. public-key certificate.

2

2. List one drawback for public key authorities [1 points]

① - need to request from the uthoritie very time you need a public key.

1 - data can be forgen and tampered easly.

3. What is the probability of finding a collision for an ideal 60-bit hash function? What is the main reason for this probability? [2 points]

1 probability is 0,5 ≥, based on birth day attack ther is will be 2 persons from 23 having same birth day.

4. Explain the birthday attack by an adversary whom wishes to find two messages or data blocks, x and y, that yield the same hash function: H(x) = H(y). [3 points]

- first generat $2^{m/2}$ x' message having same meaning of the orginel

✗ hashed the $2^{m/2}$ messages y'

2'2 - the probability to find message $H(x) = H(y)$ is 50%

on average time $2^{m/2}$ wher m is number of bits of the hash.

5. Detail what is the difference between a Hash Function and a Cryptographic Hash Function? [2 points]

in addition to Hash Function.

- Cryptographic Hash function is require to:

① infeasable to get two messages with same hash.

② one-way method so the orginel text cant resolve from hash.

2 ③ if its encrypted can provide MAC or. signeture.

- Hash function:

① detict chonges in message.

② has fixed length value.

Part 4:

1. List two of the four protocols of the SSL protocol? [1 points]

- SSL handshake protocal
- SSL Change Crypto spec protocol

1 ✓

2. In SSL handshake, the last phase sends *finished_message* from client to server. What is the main content and purpose of this message. [2 points]

is contain hash of all previous phases, so the server can check if every thing is correct or not, then server send finishe message.

2 ✓

3. What is the purpose of the dual signature in SET protocol? [2 points]

by using dual signature the customer can concatinate both the hashes of order info, and Pament Info., so marchament or bank can varific both messages.

2

4. What is HTTPS Protocol? [1 point]

It's combination of HTTP request with SSL protocal with provide secure communication by encripting all passed data.

1 ✓

5. In SET protocol, the merchant forwards to the payment Gateway (bank) encrypted blocks of related payment information sent by the cardholder. What do the encrypted blocks contain? and what type of verification the payment gateway performs from it? [2 points]

It's contain payment information and hash of order Information and the dual signature, so bank when decrypte the message can varifie that this payment information is belong to the order hash or not.

2 ✓

6. Suppose an attacker records an entire SSL session between a bank and a bank customer. Can the attacker replay the session to the bank, and potentially cause the customer to pay the same bill twice? If yes, explain why. If not, briefly explain what prevents this form of replay in SSL. [2 marks]

no, because new SSL session is encrypted using temp key, so when the attacker estaplish new SSL connection a new temp key is will used in the SSL session so replay the same session is will not work.

2 ✓